SAFER SECURITY ALERT FOR ENTERPRISE RESOURCES

Volume 3 Issue 6 **June 2000**

The Relay Group produces this newsletter to aid and assist security-concerned executives and IT professionals. The Relay Group's comments are opinions only. No action may be taken against The Relay Group for following comments or for any consequence of action emanating from the reading of this newsletter.

SAFER subscriptions can be made at http://www.safermag.com

CONTENTS

EXECUTIVE NEWS

What follows is the author's selection of rumors and noises of concern to the security community. We welcome your comments and opinions.

General News

- **A computer virus dubbed the "Love Bug" caused havoc** with computer systems worldwide, shutting down email servers at major companies and penetrating the Pentagon and Britain's parliament. Companies across Europe, North America, Asia and Australia are said to have been hit by the virus, raising fears of a repeat of the Melissa virus which caused chaos in the United States last year. The world's biggest wireless telecom firm, Vodafone AirTouch Plc (VOD), shut down its email system because of the "Love Bug" and London's House of Commons also succumbed and closed its email system for about two hours while it eradicated it. "We've got the 'I Love You' virus," a Vodafone spokesman told Reuters in London. "It's very widespread and I believe many of the major corporations are affected." The new virus originates in an email entitled "I love you" and reading: "kindly check the attached LOVELETTER coming from me." Once the attachment is launched, the virus sends copies of the same email to everybody in the user's address book. It targets Microsoft (MSFT) Corp's Outlook software and works on the same principle as the Melissa virus, which infected about a million computers, clogging whole networks in the United States and causing $80 million in damage in early 1999. Of course, everybody fails to mention that it is user who clicks on the attachment that activates the virus.
- **Governments are moving too slowly to tackle the rising tide of cyber crime**, according to lobby groups and industry bodies at the G8 conference on computer criminals. High-tech companies say governments will need their help to beat fraudsters, virus writers, malicious hackers and perpetrators of other cyber crimes. But the firms are resisting attempts to turn them into surrogate police forces and say governments need to do more by themselves. The Council of Europe is drafting an international convention to fight hackers, virus writers and Internet fraudsters. But the convention, which is also getting input from non-EU members Japan, United States, Canada and South Africa, will not be ready for signing before September 2001.

Europe – Middle-East

- **A few weeks back, Russia's secret service agency** raised privacy watchdogs' hackles when it admitted it could intercept and monitor all Russian Internet traffic. On Sunday the British government acknowledged that it was building a system that could do the same thing in Great Britain, ostensibly to help catch money launderers, terrorists, pedophiles, and other criminals who do business online. It also could help usher in an era of Orwellian surveillance, privacy advocates fear. "They've taken a lead from the KGB," said Jason Catlett, president of Junkbusters, an online privacy advocacy group. The British system, called the Government Technical Assistance Centre, will have its hub in the headquarters of the MI5, the British secret service agency. All of Britain's Internet Service Providers will be connected to the GTAC through dedicated lines (which they will have to pay for themselves). After its scheduled completion by the end of the year, the system will allow British police and secret service agents to intercept every bit of the country's Internet traffic. That could include email, credit card transactions, banking data -- any information exchanged between computers on the Web. Why are all privacy attacks by governments justified by "catching terrorists" phrase, and yet we have failed to see any government catching terrorists just by looking at Internet traffic.
- **The number of computer-related crimes continues to rise in Russia**, with more than 200 cases of hacking reported in the first three months of the year, a news agency quoted a top police official. More computer crimes were recorded in the period from January through March than in all of 1999, said Vitaly Degterev, first deputy chief of the Interior Ministry's department on high-tech crimes.

- **The European ministers of Foreign Affairs are expected to decide** to lift all barriers to the export of encryption software to countries outside the European Union. Till now, companies wanting to export encryption products had to ask for permission. The authorities first investigated if the buyer was 'secure'. Intelligence services also investigated the products, which made it possible to copy the keys or demand weakening of the encryption standard as a condition for approval. Decisions could drag on for months, which hampered the trade in encryption software. Besides that, the European industry has asked repeatedly for secure and good encryption, as a condition to boost ecommerce. They want to develop, use and export their own encryption products, as there is mistrust towards American encryption products which are believed to be weakened by the American intelligence agencies, or have secret backdoors. According to the spokesman of commissioner Liikanen of the Information Society, secret services still can ask companies to the destination of their export.

United States - Canada

- **Adding new teeth to federal laws governing high-tech crime**, the U.S. Sentencing Commission has sent Congress guidelines for judges that would substantially increase penalties for such crimes as credit card and identity theft, using computers to solicit or sexually exploit minors and violating copyrights or trademarks online. Most of the new standards will take effect Nov. 1 unless Congress strikes them, which it rarely does. The copyright and trademark provisions take effect immediately because Congress gave the commission authority to act quickly to stem a practice that one trade association estimated costs the software industry $11.4 billion each year.
- **Consumers who have bought into a phony investment scheme on the Internet** or who have had strange charges appear on their credit card statements after buying something through a Web site can now report the crime online. With literally a click, victims can send an e-mail to local, state and federal officials if they think they have been the victim of a scam or theft through the Internet. The Internet Fraud Complaint Center (IFCC), launched by the FBI and the Virginia-based National White Collar Crime Center, will help law enforcement and regulators track and investigate cases of Internet fraud as Americans start to spend more time in cyberspace.
- **Opening a political can of worms, the Federal Trade Commission** today said it would embark on a major policy shift, asking Congress to enact stronger legislation to oversee online privacy. The commission voted 3-2 to release a report concluding that "legislation is necessary" to ensure Internet privacy protections and that "industry alone have not been sufficient." That position is in marked contrast to the agency's prior stance, endorsed by the Clinton administration, of allowing corporate self-regulation on privacy. Although privacy legislation is unlikely to come this year, the commission's change in focus could put new pressure on policy-makers and might even play a role in the upcoming presidential contest between Vice President Al Gore and Texas Gov. George W. Bush, experts said.

Asia - Pacific

- **China has toughened regulations against computer viruses**, mandating fines and up to five years imprisonment for people who spread the bugs, an official newspaper reported. The China Daily said the regulations were issued by the Ministry of Public Security and were made public, after the ILOVEYOU virus crippled e-mail systems worldwide. The regulations require “workplaces using computers” to install virus prevention systems, scan their computer networks, train their workers on how to prevent viruses and only use officially authorized anti-virus products, the newspaper said. The report also said people will be fined up to $3,600 for spreading viruses “if commercial operations are involved.” Violators could also face maximum prison terms of five years, it said.

SECURITY ALERTS

We try to inform you of vulnerabilities as soon as they become a threat to your resources, not when the vendors decide to report them.

Initialized Data Overflow in Xlock

Released May 29, 2000

Affects All systems running xlock

Reference http://www.nai.com/covert

Problem

- An implementation vulnerability in xlock allows global variables in the initialized data section of memory to be overwritten.
- This creates the potential for local users to view the contents of xlock's memory, including the shadowed password file, after root privileges have been dropped.

SAFER

- Patches for most UNIX distributions (and source code) have been released.

Linux cdrecord Buffer Overflow Vulnerability

Released May 27, 2000

Affects Linux Mandrake 7.0

Reference http://www.securityfocus.com/bid/1265

Problem

- The linux cdrecorder binary is vulnerable to a locally exploitable buffer overflow attack. When installed in a Mandrake 7.0 linux distribution, it is by default setgid "cdburner" (which is a group, gid: 80, that is created for the application). The overflow condition is the result of no bounds checking on the 'dev=' argument passed to cdburner at execution time.
- This vulnerability can be exploited to execute arbitrary commands with egid "cdburner". cdburner has been verified (by the writers of the exploit) to be exploitable on an Intel linux system running Mandrake 7.0. Other distributions of linux may be vulnerable to this problem as well.
- If system has SCSI hard disks, user might be able to gain access to raw disk device and gain root privileges or render system unstable.

SAFER

- A workaround (until an official patch is released) is to remove the setgid bit from the cdburner binary.

KDE kdesud DISPLAY Environment Variable Overflow

Released May 27, 2000

Affects KDE 1.2, 1.1.2, 1.1.1, 1.1

Reference http://www.securityfocus.com/bid/1274

Problem

- /usr/bin/kdesud has a DISPLAY environment variable overflow which could allow for the execution of arbitrary code.

SAFER

- Patch has been released.

Security Vulnerability in IPFilter 3.3.15 and 3.4.3

Released May 26, 2000

Affects IPFilter 3.3.15 and 3.4.3

Reference **http://www.prettyhatemachine.obfuscation.org/**

Problem

- A weakness exists in the IPFilter firewalling package in all versions up to and including 3.3.15 and 3.4.3 that allows an attacker to penetrate the firewall when a common, yet admittedly flawed, configuration is used.

SAFER

- A patch has been made available for all versions of IPFilter. It is also important to note that kind of 'misconfiguration' is required on admin side in order to make this vulnerability work.

Microsoft Windows Long Filename Extension Vulnerability

Released May 26, 2000

Affects Microsoft Windows 98, 95

Reference **http://www.securityfocus.com/bid/1259**

Problem

- Windows 95 and 98 suffer from a buffer overflow that will result in a crash if a filename with an extension longer that 232 characters are accessed. Although arbitrary code could be executed via this manner, it would have to be composed of valid filename character values only.

SAFER

- Windows NT 4.0 has not yet been tested for this vulnerability, and therefore may be vulnerable as well.

PDGSoft Shopping Cart Multiple Buffer Overflow Vulnerabilities

Released May 25, 2000

Affects PDGSoft Shopping Cart 1.50

Reference **http://www.securityfocus.com/bid/1256**

Problem

- The two executables with the vulnerabilities are redirect.exe (redirect.cgi on UNIX) and changepw.exe (hangepw.cgi on UNIX), both of which are accessible over the web.
- If supplied an overly long query string both will overflow an internal buffer overwriting the saved return address.

SAFER

- The vendor has made available a patch for every affected platform.

Network Associates WebShield SMTP 4.5.44 Buffer Overflow Vulnerability

Released May 25, 2000

Affects Network Associates WebShield SMTP 4.5.44

Reference **http://www.securityfocus.com/bid/1254**

Problem

- Network Associates WebShield SMTP is susceptible to a buffer overflow attack if 208 or more bytes of data accompanying a configuration parameter are transmitted to the remote management service listening at port 9999.
- It is possible to force the program to execute arbitrary code at the privilege level of the service's account (default SYSTEM).

SAFER

- Run the application as a restricted user account rather than as SYSTEM and disable the management service.

Omnis Studio 2.4 Weak Database Field Encryption Vulnerability

Released May 25, 2000

Affects Omnis Studio 2.4

Reference **http://www.securityfocus.com/bid/1255**

Problem

- The encryption scheme used in Omnis Studio is weak and easily broken with any scientific calculator or even pen and paper, if the attacker has a good knowledge of hex and ASCII. Each unencrypted byte is simply replaced with a value dependent on that byte's original value and the remainder of its position in the string divided by 4.
- Note that this vulnerability does not affect the security of Omnis Studio directly, but will be present in all applications designed using Omnis Studio.

SAFER

- No responses from the vendor yet.

Network Associates WebShield SMTP 4.5.44 Configuration Modification Vulnerability

Released May 25, 2000

Affects Network Associates WebShield SMTP 4.5.44

Reference **http://www.securityfocus.com/bid/1253**

Problem

- By default, Network Associates WebShield SMTP runs the management agent on port 9999. A remote user may gain access to this agent and modify the configuration of WebShield SMTP simply by connecting to this particular port. Issuing the command "GET_CONFIG<CR>" will return the current configuration.
- The management agent grants access based on a list of authorized hostnames, but will grant access to any IP address which cannot be resolved to a hostname even if 'MailCfg' is set to only allow configuration from localhost.

SAFER

- This vulnerability is not present in Network Associates WebShield SMTP 4.5.74.0 or later. It is recommended to upgrade to version 4.5.74.0 or later.

HP Web JetAdmin Directory Traversal Vulnerability

Released May 24, 2000

Affects HP JetAdmin 5.6, HP JetAdmin 5.5.177

Reference **http://www.securityfocus.com/bid/1243**

Problem

- By default JetAdmin Web Interface Server listens on port 8000. By requesting a specially formed URL which includes "../" it is possible for a remote user to gain read-access to any files outside of the web-published directory.

SAFER

- Upgrade to Version 6.0.

Qualcomm Qpopper 'EUIDL' Format String Input Vulnerability

Released May 24, 2000

Affects Qualcomm qpopper 2.53, 2.52

Reference **http://www.securityfocus.com/bid/1242**

Problem

- By placing machine executable code in the X-UIDL header field, supplying formatting strings in the "From:" field in a mail header, and then issuing, as the user the mail was sent to, a 'euidl' command, it is possible to execute arbitrary code.
- This code will execute as the user executing the euidl command, but with group 'mail' permissions on hosts running qpopper in that group. This is often done due to mail spool permissions.
- This vulnerability does not exist in versions after 2.53. It also requires an account on the machine.

SAFER

- The vendor recommends upgrading to versions 3.0.2 or later of qpopper.

MDBMS Buffer Overflow Vulnerability

Released May 24, 2000

Affects MDBMS .9xbx

Reference **http://www.securityfocus.com/bid/1252**

Problem

- By supplying a line of sufficient length to the MDBMS server, containing machine executable code, it is possible for a remote attacker to execute arbitrary commands as the user the db is running as.
- It is believed all versions of MDBMS are susceptible, up to and including .99b6, which is the latest release.

SAFER

- Unofficial patch is available.

MailSite 4.2.1.0 Buffer Overflow Vulnerability

Released May 24, 2000

Affects MailSite 4.2.10

Reference **http://www.securityfocus.com/bid/1244**

Problem

- Remote users are able to execute arbitrary code with system privileges by exploiting a buffer overflow vulnerability that exists in the code that handles GET requests in Rockliffe MailSite 4.2.1.0.
- Performing a GET request containing a query string consisting of over 240 KB will allow for the execution of arbitrary code.

SAFER

- Rockliffe has rectified this vulnerability with the release of MailSite 4.2.2.

Pacific Software Carello File Duplication and Source Disclosure Vulnerability

Released May 24, 2000

Affects Pacific Software Carello 1.2.1

Reference **http://www.securityfocus.com/bid/1245**

Problem

- A remote user can gain read and write access on a target machine running Carello shopping cart software.
- A user may create a duplicate of a known file in a known directory on the target host through add.exe in /scripts/Carello.
- Accessing *http://target/scripts/Carello/add.exe?C:\directory\filename.ext* will generate a duplicate file with a "1" appended to the filename (eg. filename.ext1). From here, the remote user would perform a http request of the newly created duplicate file and be able to view the contents of it.
- This vulnerability depends on the anonymous internet account having write access to the relevant directories.

SAFER

- Disable access to sensitive directories for the anonymous internet account.

PGP5i Automatic Key Generation Routine Vulnerability

Released May 24, 2000

Affects PGPi 5.0i

Reference http://www.securityfocus.com/bid/1251

Problem

- Vulnerability exists in the way PGP5i generates random keying material, when used without user input. When a keypair is generated using: pgpk -g <DSS or RSA> <key-length> <user-id> <timeout> <pass-phrase> pgp will automatically generate the key without any user intervention. On systems which support /dev/random, it generates this key material by reading from this device in 1 byte increments: RandBuf = read(fd, &RandBuf, count); which it then feeds in to its random pool. Unfortunately, the above logic is flawed; read() returns the number of characters read.
- As count is always initialized to 1 in this case, RandBuf will always be assigned the value 1. This makes it easy to predict keys. RSA keys generated this way are predictable; DSA/ElGamal signature (DSA) keys are predictable, while encryption keys (ElGamal) vary.

SAFER

- Upgrade your PGPi 5.0i to PGPi 6.5.

NetOp Remote Control Unauthenticated File Transfer Vulnerability

Released May 23, 2000

Affects Data NetOp 6.50, 6.0

Reference http://www.securityfocus.com/bid/1263

Problem

- NetOp is a remote control utility, offering console access via network or serial connections. On NT and Windows 2000 machines, the software runs in the SYSTEM context by default. The software includes the ability to perform direct file transfers to and from the host machine.
- No authentication is required to perform this activity, meaning that any user with the freely downloadable client and access to netbios sessions on the target can perform read/write/create operations to any file on the system, including password and configuration data.

SAFER

- NetOp version 6.50 has the ability to use either NetOp or Windows security to authenticate users immediately upon connection, although this is not enabled by default.

Cayman 3220H DSL Router "ping of death" Vulnerability

Released May 23, 2000

Affects Cayman 3220-H DSL Router 1.0, GatorSurf 5.5Build R1, R0, 5.3build R2, R1

Reference http://www.securityfocus.com/bid/1240

Problem

- Sending an oversized ICMP echo request to the router can cause a denial of service. Reported effects vary; sometimes it stops telnet and http admin services, other times the router may restart without routing but the admin services stay up.

SAFER

- Update has been released by the vendor.

Cobalt RaQ2/RaQ3 Web Server Appliance cgiwrap bypass Vulnerability

Released May 23, 2000

Affects Cobalt RaQ 3.0, 2.0

Reference **http://www.securityfocus.com/bid/1238**

Problem

- There is a security problem with FrontPage extensions on the Cobalt RaQ2 and RaQ3 web hosting appliances. It allows any user on the system to change, delete, or overwrite a FrontPage site.
- When a site is uploaded with FrontPage to a RaQ2/3, all of the files are owned by user "httpd" instead of a site-specific user. The Apache web server is also running as user "httpd". Cobalt uses cgiwrap to have CGIs run as the user that owns the CGI instead of "httpd", but it is trivial to bypass cgiwrap and run scripts as user "httpd".

SAFER

- Cobalt Networks has released patches for the RaQ 3i and RaQ 2 which fix this issue.

GNOME gdm XDMCP Buffer Overflow Vulnerability

Released May 22, 2000

Affects gdm 2.0.x BETA, 1.0.x

Reference **http://www.securityfocus.com/bid/1233**

Problem

- A buffer overrun exists in the XDMCP handling code used in 'gdm', an xdm replacement, shipped as part of the GNOME desktop. By sending a properly crafted XDMCP message, it is possible for a remote attacker to execute arbitrary commands as root on the susceptible machine. The problem lies in the handling of the display information sent as part of an XDMCP 'FORWARD_QUERY' request.
- By default, gdm is not configured to listen via XDMCP. The versions of gdm shipped with RedHat 6.0-6.2, Helix GNOME and gdm built from source are not vulnerable unless they were configured to accept XDMCP requests. This is configured via the /etc/X11/gdm/gdm.conf on some systems, although this file may vary. If the "Enable" variable is set to 0, you are not susceptible.

SAFER

- Changing the contents of the 'Enable' variable to 0 in the gdm configuration file (often /etc/X11/gdm/gdm.conf) will eliminate this vulnerability.

Multiple Linux Vendor fdmount Buffer Overflow Vulnerability

Released May 22, 2000

Affects S.u.S.E. Linux, Slackware Linux, Turbo Linux

Reference **http://www.securityfocus.com/bid/1239**

Problem

- A buffer overflow exists in the 0.8 version of the fdmount program, distributed with a number of popular versions of Linux. By supplying a large, well crafted buffer containing machine executable code in place of the mount point, it is possible for users in the 'floppy' group to execute arbitrary commands as root.
- This vulnerability exists in versions of S.u.S.E., 4.0 and later, as well as Mandrake Linux 7.0. TurboLinux 6.0 and earlier ships with fdmount suid root, but users are not automatically added to the 'floppy' group. This list is by no means meant to be complete; other Linux distributions may be affected. To check if you're affected, check for the presence of the setuid bit on the binary. If it is present, and the binary is either world executable, or group 'floppy' executable, you are affected and should take action immediately.

SAFER

- MandrakeSoft has provided a source patch to this problem. It is expected that both MandrakeSoft and SuSE will release RPM's to fix this problem shortly. A suitable solution may be to remove the setuid bit on the fdmount binary, or remove non-trusted users from the 'floppy' group.

MetaProducts Offline Explorer Directory Traversal Vulnerability

Released May 19, 2000

Affects MetaProducts Offline Explorer 1.2x, 1.1x, 1.0x

Reference http://www.securityfocus.com/bid/1231

Problem

- By default Offline Explorer listens on port 800 on which a remote user can gain read-access to a remote host's web cache and from their directory traverse.
- Performing a GET request containing "../..\" will allow the remote user to browse the cache and the upper directory structure.

SAFER

- Download latest version of Offline Explorer.

Gauntlet Firewall Remote Buffer Overflow Vulnerability

Released May 19, 2000

Affects Gauntlet Firewall 5.5, 5.0, 4.2, 4.1, WebShield E-ppliance 300.0, 100.0

Reference http://www.securityfocus.com/bid/1234

Problem

- A buffer overflow exists in the version of Mattel's Cyber Patrol software integrated in to Network Associates Gauntlet firewall, versions 4.1, 4.2, 5.0 and 5.5. Due to the manner in which Cyber Patrol was integrated, a vulnerability was introduced which could allow a remote attacker to gain root access on the firewall, or execute arbitrary commands on the firewall.
- By default, Cyber Patrol is installed on Gauntlet installations, and runs for 30 days. After that period, it is disabled. During this 30 day period, the firewall is susceptible to attack. Due to the filtering software being externally accessible, users not on the internal network may also be able to exploit the vulnerability

SAFER

- Patches from NAI are available.

Lotus Domino Server Misconfiguration: Documents Can Be Modified over the Web

Released May 19, 2000

Affects Lotus Domino Server

Reference http://www.perfectotech.com/blackwatchlabs/

Problem

- Documents (records) available for viewing in Lotus Domino server may be edited over the web, if the access rights are not properly configured for them.
- The access rights for documents available through Lotus Domino server allow users to edit them, although the URL contains only the “open” (i.e. view) operation. This can be done easily via modifying the URL, so that instead of “OpenDocument”, the browser will send “EditDocument”.

SAFER

- Each site running a Domino server is encouraged to ensure that its databases are well-configured, so that the outside user is not allowed to change records.

Big Brother bbd.c Buffer Overflow Vulnerability

Released May 18, 2000

Affects Big Brother 1.0 up to 1.4

Reference http://www.securityfocus.com/bid/1257

Problem

- Big Brother versions prior to 1.4g (BBDisplay and BBPager bbd.c) contain a buffer overflow vulnerability, which allows for the execution of arbitrary code with the permissions of the user running bbd.c

SAFER

- Download and install version 1.4g.

Lotus Domino Server ESMTP Buffer Overflow Vulnerability

Released May 18, 2000

Affects Lotus Domino Enterprise Server and Mail Server 5.0.3, 5.0.2, 5.0.1

Reference **http://www.securityfocus.com/bid/1229**

Problem

- The code that handles the 'from' command in the ESMTP service of Lotus Domino Server 5.0.1 has an unchecked buffer.
- If Lotus Domino Server receives an argument of more than 4 KB to the 'from' command, the system will crash and will require a reboot in order to regain normal functionality.

SAFER

- No patches have been issued by Lotus/IBM. There are no known workarounds.

FreeBSD and Linux Mandrake 'xsoldier' Buffer Overflow Vulnerability

Released May 17, 2000

Affects FreeBSD 3.3, Linux Mandrake 7.0

Reference **http://www.securityfocus.com/bid/871**

Problem

- Certain versions of FreeBSD (3.3 Confirmed) and Linux (Mandrake confirmed) ship with a vulnerable binary in their X11 games package. The binary/game in question, xsoldier, is a setuid root binary meant to be run via an X windows console.
- The binary itself is subject to a buffer overflow attack (which may be launched from the command line) which can be launched to gain root privileges. The overflow itself is in the code written to handle the -display option and is possible overflow by a user supplied long string.
- The user does not have to have a valid $DISPLAY to exploit this.

SAFER

- Update for Mandrake is available.

NetworkICE ICECap Manager Default Username and Password Vulnerability

Released May 17, 2000

Affects NetworkICE ICECap Manager 2.0.23 and previous

Reference **http://www.securityfocus.com/bid/1216**

Problem

- By default, ICECap Manager listens on port 8081, transmits alert messages to another server on port 8082, and has an administrative username of 'iceman' possessing a blank password. A remote user could login to ICECap manager through port 8081 (using the default username and password if it hasn't been modified) and send out false alerts.
- In addition, the evaluation version of ICECap Manager has the option of utilizing Microsoft Access' JET Engine 3.5. This creates a security hazard because JET Engine 3.5 is vulnerable to remote execution of Visual Basic for Application code. Therefore, remote users may execute arbitrary commands on ICECap Manager through the use of the default username and password and JET Engine 3.5.

SAFER

- NetworkICE has released ICECap Manager 2.0.23a which rectifies this issue.

KDE kscd SHELL Environmental Variable Vulnerability

Released May 16, 2000

Affects KDE 2.0 BETA, 1.2, 1.1.1, 1.1

Reference **http://www.securityfocus.com/bid/1206**

Problem

- Some linux distributions (S.u.S.E. 6.4 reported) ship with kscd (a CD player for the KDE Desktop) sgid disk. kscd uses the contents of the 'SHELL' environment variable to execute a browser. This makes it possible to obtain an sgid 'disk' shell.
- Using these privileges along with code provided in the exploit, it is possible to change attributes on raw disks. This in turns allows an attacker to create a root shell, thus compromising the integrity of the machine.
- Red Hat, Linux Mandrake, and Turbo Linux do not currently ship with kscd setgid 'disk'.

SAFER

- Removal of the sgid bit on the kscd binary will eliminate this vulnerability.

Matt Kruse Calendar Arbitrary Command Execution Vulnerability

Released May 16, 2000

Affects Matt Kruse Calendar Script 2.2

Reference **http://www.securityfocus.com/bid/1215**

Problem

- There are two components of this package, calendar-admin.pl and calendar.pl. Calendar-admin.pl calls open() with user-input in the command string but does not parse the input for metacharacters. It is therefore possible to execute arbitrary commands on the target host by passing "|shell command|" as one value of the "configuration file" field.
- The shell that is spawned with the open() call will then execute those commands with the uid of the webserver. This can result in remote access to the system for the attacker. Calendar.pl is vulnerable to a similar attack.

SAFER

- New version of Calendar is available.

Netopia DSL Router Vulnerability

Released May 16, 2000

Affects Netopia R-series routers 4.6.2

Reference **http://www.securityfocus.com/bid/1177**

Problem

- All R-series platforms with firmware between 4.3.8 and 4.6.2 (inclusive) allow users who already have access to the router to modify SNMP tables which they should not be able to access. The router has a command-line mode that is reached by typing control-N after the user has passed the initial login test.
- At the "#" prompt one can then do most management of the device. This includes the setting of SNMP community strings in spite of the limitation imposed by the administrator.

SAFER

- Download version 4.6.3 of the firmware.

Multiple Vendor Kerberos 5/4 Compatibility krb_rd_req() Buffer Overflow Vulnerability

Released May 16, 2000

Affects MIT Kerberos

Reference **http://www.securityfocus.com/bid/1220**

Problem

- Several buffer overflow vulnerabilities exist in Kerberos 5 implementations due to buffer overflows in the Kerberos 4 compatibility code. These include MIT Kerberos 5 releases 1.0.x, 1.1 and 1.1.1, MIT Kerberos 4 patch level 10 (and, most likely, prior releases), and Cygnus KerbNet and Network Security (CNS).
- The main source of problems is due to a buffer overflow in the krb_rd_req() library function. This function is used by every application that supports Kerberos 4 authentication, including, but not limited to, kshrd, klogin, telnetd, ftpd, rkinitd, v4rcp and kpopd. Therefore, it is possible for a remote attacker to exploit this vulnerability and gain root access on affected machines, or obtain root level access once local.
- A setuid version of v4rcp is shipped with RedHat Linux 6.2, as part of a full install. It is possible to use this program, to obtain root level access.
- In addition, there are other buffer overruns present in the ksu and krshd sources from MIT. These problems will be remedied in the same release from MIT that fixes the krrb_rd_req() vulnerability.

SAFER

- Various patches/updates are available.

Hot Area Banner Rotation World-Readable Password Vulnerability

Released May 16, 2000

Affects Hot Area Banner Rotation 1.0

Reference **http://www.securityfocus.com/bid/1218**

Problem

- Hot Area Banner Rotation 01 and Dream Catcher Advertiser stores its administrative password in the file adpassword.txt. Although the password is DES encrypted, it is world-readable by any remote user.
- Thus, a password cracker could be used by a malicious to decrypt it. By default, the password is 'admin' and appears DES encrypted as 'aaLR8vE.jjhss' in adpassword.txt.
- Administrative controls include editing, removing, and adding of advertisement banners.

SAFER

- Set access controls on the file adpasswd.txt to prevent users from retrieving it.

AntiSniff DNS Overflow Vulnerability

Released May 16, 2000

Affects AntiSniff 1.0.1, AntiSniff - Researchers Version 1.0

Reference **http://www.securityfocus.com/bid/1207**

Problem

- Certain versions of @Stake Inc.'s Antisniffer software contain a remotely exploitable buffer overflow. AntiSniff is a program that was released by L0pht Heavy Industries in July of 1999. It attempts, through a number of tests, to determine if a machine on a local network segment is listening to traffic that is not directed to it (commonly referred to as sniffing).
- During one particular test there is a problem if a packet that does not adhere to DNS specifications is sent to the AntiSniff machine. This can result in a buffer overflow on the system running AntiSniff. If the packet is crafted appropriately this overflow scenario can be exploited to execute arbitrary code on the system.
- This scenario is only possible if AntiSniff is configured to run the DNS test and only during the time the test is running. Nonetheless, it is a vulnerability that should not be ignored and has even been found in other promiscuous mode detection programs as well.

SAFER

- Do not run the DNS tests on AntiSniff version 1.01 or the Researchers version 1.0.

Seattle Lab Emurl 2.0 Email Account Access Vulnerability

Released May 15, 2000

Affects Seattle Lab Software Emurl 2.0

Reference **http://www.securityfocus.com/bid/1203**

Problem

- Emurl software creates a unique identifier for each user, based on their account name. This identifier is encoded using the ascii value of each character in the account name and augmented by its position.
- By using a specific URL along with a user's identifier, it is possible to retrieve that users e-mail as well as view and change their account settings.

SAFER

- Seattle Lab is aware of the issue and will address it in their next version of Emurl.

Qualcomm Eudora Pro Long Filename Attachment Vulnerability

Released May 15, 2000

Affects Qualcomm Eudora 4.3, 4.2, Eudora Light 3.0, Eudora Pro 1.0

Reference **http://www.securityfocus.com/bid/1210**

Problem

- Eudora improperly handles filenames of files attached in e-mails. An exceedingly long filename can result in a buffer overflow condition when the program processes the attachment and tries to save the temporary file.
- In Eudora e-mail is processed while downloading mail from the server so buffer overflow occurs when the message is processed from the spool directory. This can even lock the e-mail account of the Eudora user. Attacker-supplied data makes it into EIP, so execution of arbitrary remote code is a possibility.

SAFER

- Deleting the offending file from the attachment directory under a DOS prompt reportedly allows Eudora to regain functionality.

CGI Counter Input Validation Vulnerability

Released May 15, 2000

Affects CGI Counter 4.0.7, 4.0.2

Reference **http://www.securityfocus.com/bid/1202**

Problem

- Due to unchecked code that handles user input in George Burgyan's CGI Counter, remote execution of arbitrary commands at the same privilege level as the web server it is running on is possible.

SAFER

- Use other counter program/script.

Microsoft Active Movie Control Filetype Vulnerability

Released May 13, 2000

Affects Microsoft Active Movie Control 1.0

Reference **http://www.securityfocus.com/bid/1221**

Problem

- The Microsoft Active Movie Control (a multimedia ActiveX control) will download files of any type specified in the control parameters in an HTML document, regardless of whether or not they are a valid media type.
- A hostile website, HTML email or HTML newsgroup post could therefore write executables and other potentially harmful content to target machines, which will be stored with their known filenames in the default Windows Temp directory.
- This vulnerability could be used in conjunction with other exploits to run arbitrary code on the target machine(s).

SAFER

- Disable Active Scripting.

Solaris netpr Buffer Overflow Vulnerability

Released May 12, 2000

Affects Sun Solaris 2.6, 7.0, 8.0

Reference **http://www.securityfocus.com/bid/1200**

Problem1

- A buffer overrun exists in the 'netpr' program, part of the SUNWpcu (LP) package included with Solaris, from Sun Microsystems. Versions of netpr on Solaris 2.6 and 7, on both Sparc and x86 have been confirmed as being vulnerable.
- The overflow is present in the -p option, normally used to specify a printer. By specifying a long buffer containing machine executable code, it is possible to execute arbitrary commands as root. On Sparc, the exploits provided will spawn a root shell, whereas on x86 it will create a setuid root shell in /tmp.

SAFER

- Sun has patches available for this vulnerability.

Microsoft Outlook 98 / Outlook Express 4.x Long Filename Vulnerability

Released May 12, 2000

Affects Microsoft Outlook 98, Microsoft Outlook Express 4.0 up to 4.72.3612.1700

Reference **http://www.securityfocus.com/bid/1195**

Problem

- When the email client receives a malicious mail or news message that contains an attachment with a very long filename, it could cause the email client to shut down unexpectedly. These very long filenames do not normally occur in mail or news messages, and must be intentionally created by someone with malicious intent. A skilled hacker could use this malicious email message to run arbitrary computer code contained in the long string.
- This issue can cause one of the following to occur when attempting to download, open or view an mail or news message in Microsoft Outlook 98 or Microsoft Outlook Express 4.x that has an attachment with a very long filename.
- An error message similar to the following may be displayed: This program has performed an illegal operation and will be shut down. If the problem persists, contact the program vendor. This issue does not affect outlook Express 4.01 for Microsoft Windows 3.1 and Windows NT 3.51.

SAFER

- Microsoft has released patches to fix Outlook 98 and Outlook Express 4.x.

Microsoft Office 2000 UA Control Vulnerability

Released May 11, 2000

Affects Microsoft Office 2000

Reference **http://www.securityfocus.com/bid/1197**

Problem

- Microsoft Office 2000 and related individual packages (eg., Microsoft Word 2000) have a feature called "Show Me" as part of the built-in help, which makes use of an ActiveX control (Office 2000 UA Control).
- This function was incorrectly flagged as "safe for scripting" and, although undocumented, could be used by a malicious web site operator to execute any commands in Microsoft Office 2000. It provides the ability to script almost all Office 2000 functions including file manipulation, configuration settings, etc.

SAFER

- Microsoft has released a patch which fixes this vulnerability.

NTMail Server 5.x Proxy Access Vulnerability

Released May 12, 2000

Affects NTMailserver.com NTMail 5.0

Reference **http://www.securityfocus.com/bid/1196**

Problem

- NTMail server can be configured as a proxy server as well as a web configuration server. By default each function is assigned a port. The configuration function uses port 8000 and the proxy function uses port 8080.
- If a separate proxy server is being utilized with security restrictions in place, it is possible to disable the proxy function of the NTMail server, thus forcing users to go through the restricted proxy server. However a user could reconfigure their proxy setup to point to NTMail on port 8000, redirecting them to the internet with no restrictions.

SAFER

- Disable the WWW configuration service until a patch is released.

Microsoft IIS 4.0/5.0 Malformed Filename Request Vulnerability

Released May 11, 2000

Affects Microsoft IIS 4.0, 5.0

Reference **http://www.securityfocus.com/bid/1193**

Problem

- Requesting a known filename with the extension replaced with .htr preceded by approximately 230 "%20" (which is an escaped character that represents a space) from Microsoft IIS 4.0/5.0 will cause the server to retrieve the file and its contents. This is due to the .htr file extension being mapped to ISM.DLL ISAPI application which redirects .htr file requests to ISM.DLL. ISM.DLL removes the extraneous "%20" and replaces .htr with the proper filename extension and reveals the source of the file.
- This action can only be performed if an .htr request has not been previously made or if ISM.DLL is loaded into memory for the first time. If an .htr request has already been made, a restart of the web server is necessary in order to perform another.

SAFER

- Microsoft has released patches, which rectify this issue.

Bugzilla 2.8 Unchecked Existing Bug Report Vulnerability

Released May 11, 2000

Affects Mozilla Bugzilla 2.8

Reference **http://www.securityfocus.com/bid/1199**

Problem

- The machine running bugzilla is vulnerable to exploitation due to an input validation error. When accepting a bug report, the script "process_bug.cgi" calls "./processmail" via system() argumented by a number of parameters with values originating from user input via a web-form.
- There are no checks against these values for shell metacharacters by the script before insertion into the system() call. Consequently, commands can be appended to the end of the form values and executed by /bin/sh in the manner: "value;id". The form value that is passed to system() for all bug reports is "who", shown here in this section of code from "process_bug.cgi":

SAFER

- Updated version of BugZilla has been released.

Microsoft Windows 2000 Default SYSKEY Configuration Vulnerability

Released May 11, 2000

Affects Microsoft Windows NT 2000

Reference **http://www.securityfocus.com/bid/1198**

Problem

- The default configuration of SYSKEY allows any local user to decrypt data encrypted with the Encrypted File System (EFS).
- A known vulnerability exists in Windows 2000 where the SAM database can be deleted if the system is booted with a different operating system. Upon reboot, a new SAM database is created with the Administrator account having a blank password. A malicious user can now login as Administrator and decrypt data if the recovery key resides on the system.
- The default mode SYSKEY operates in is to 'Store Startup Key Locally'. Under this mode, Windows 2000 will generate a random 128-bit system key and store it in the registry under HKLM/SYSTEM. Running SYSKEY in this mode will leave the system vulnerable to the exploit mentioned above.
- In addition, a tool called 'ntpasswd' is available which can reset the password of any local user account, including the administrator account, by modifying password hashes in the SAM database. A local user can use this tool to login as Administrator (who is the default data recovery agent in the EFS) and from there, decrypt data using the EFS.
- Domain-based accounts are not affected by this vulnerability.

SAFER

- Configure SYSKEY to operate in either 'Use a Passphrase to Unlock the System Key' or 'Store Startup Key on Floppy Disk' mode. However, this does not address an attack using the ntpasswd tool.

Zedz Consultants ssh-1.2.27-8i.src.rpm Access Verification Vulnerability

Released May 10, 2000

Affects Zedz Consultants ssh-1.2.27-8i.src.rpm 1.2.27-8i

Reference **http://www.securityfocus.com/bid/1189**

Problem

- A flaw exists in the RedHat Linux RPM distributed by Zedz Consulting, version 1.2.27-8i. Due to a flaw in authentication due to a patch to support PAM, it’s possible for anyone to log in to any valid account via ssh.
- This is NOT a flaw in ssh, or sshd, but rather in the patch applied in the RPM distributed. Users of SSH 1.2.27 or OpenSSH are not vulnerable to this. Only those who installed this specific RPM from the Zedz Consulting ftp site are susceptible.

SAFER

- Uninstall the rpm, and install a non-susceptible package.

Netscape Communicator /tmp Symlink Vulnerability

Released May 10, 2000

Affects Netscape Communicator 4.5 up to 4.73

Reference **http://www.securityfocus.com/bid/1201**

Problem

- Netscape Communicator version 4.73 and prior may be susceptible to a /tmp file race condition when importing certificates. Netscape creates a /tmp file which is world readable and writable in /tmp, without calling stat() or fstat() on the file. As such, it is possible, should a user be able to predict the file name, to cause a symbolic link to be created, and followed elsewhere on the file system.
- Additionally, as the file is created mode 666 prior to being fchmod()'d to 600, there may be a window of opportunity for altering the contents of this file.

SAFER

- This issue has only been demonstrated on the Linux binary, for glibc. The sparc Solaris binary does not behave this way.

Matt Wright FormMail Environmental Variables Disclosure Vulnerability

Released May 10, 2000

Affects Matt Wright FormMail 1.6

Reference **http://www.securityfocus.com/bid/1187**

Problem

- An unauthorized remote user is capable of obtaining CGI environmental variable information from a web server running Matt Wright FormMail by requesting a specially formed URL that specifies the email address to send the details to.
- This is accomplished by specifying a particular CGI environmental variable such as PATH, DOCUMENT_ROOT, SERVER_PORT in the specially formed URL which will email the results to the address given. The information obtained could possibly be used to assist in a future attack.

SAFER

- Unofficial patch is available.

Microsoft SQL Server Xp_sprintf buffer overflow

Released May 09, 2000

Affects Microsoft SQL Server 6.5, 6.0

Reference **http://www.securityfocus.com/bid/1204**

Problem

- In versions of SQL Server earlier than Release 6.5, Service Pack 5 the extended stored procedure xp_sprintf can be exploited using buffer overflows.
- An attacker can use xp_sprintf to crash the server or to possibly gain administrator privileges on the system running SQL Server.

SAFER

- This issue is resolved in version of Microsoft SQL Server greater than 6.5 SP5.

NetStructure 7180 Remote Backdoor Vulnerability

Released May 08, 2000

Affects Intel Corporation NetStructure 7180.0

Reference **http://www.securityfocus.com/bid/1183**

Problem

- This Internet equipment is designed for businesses with multiple Web site locations, routing traffic to the best available site from a single URL management. Certain revisions of this package have two undocumented supervisor passwords. These passwords are derived from is the ethernet address of the public interface which under default installs is available via a default passworded SNMP daemon.
- These passwords can be utilized via the admin console locally (via a serial interface) or remotely if the machine has been deployed with a modem for remote accessory allows telnet access. It should be noted that configuration over telnet is preferred in the user documentation. With these passwords an intruder gains shell access to the underlying UNIX system and may sniff traffic among other things.

SAFER

- Intel has provided a patch for this issue.

NetStructure 7110 Undocumented Password Vulnerability

Released May 08, 2000

Affects Intel Corporation NetStructure 7110.0

Reference **http://www.securityfocus.com/bid/1182**

Problem

- This internet equipment is designed for businesses with multiple Web site locations, routing traffic to the best available site from a single URL. Certain revisions of this package have an undocumented supervisor password. This password, which grants access to the 'wizard' mode of the device, is derived from the MAC address of the primary NIC. This MAC address is displayed in the login banner.
- This password can be utilized from the admin console locally (via a serial interface) or remotely if the machine has been deployed with a modem for remote access. With this password an intruder gains shell access to the underlying UNIX system and may sniff traffic, among other things.

SAFER

- Intel has created a patch for this issue.

AOL Instant Messenger Path Disclosure Vulnerability

Released May 08, 2000

Affects AOL Instant Messenger 4.0

Reference **http://www.securityfocus.com/bid/1180**

Problem

- If a user transmits a file through AOL Instant Messenger, the full local path of the file is displayed to the remote recipient. This information could possibly be used in order to discover the Operating System platform and other sensitive details which may assist in a future attack.

SAFER

- No details about the fix have been released. We expect that AOL will indeed fix the problem in next release or AIM.

Microsoft IIS shtml.exe Path Disclosure Vulnerability

Released May 06, 2000

Affects Microsoft FrontPage Server Extensions Module for Apache 3.0.43, IIS 4.0 and 5.0

Reference **http://www.securityfocus.com/bid/1174**

Problem

- The local path of a HTML, HTM, ASP, or SHTML file can be disclosed in Microsoft IIS 4.0/5.0. Passing a path to a non-existent file to the shtml.exe program will display an error message stating that the file cannot be found accompanied by the full local path to the web root.

SAFER

- Microsoft is aware of the issue and stated on May 8, 2000 that a patch is forthcoming.

Netwin DNews News Server Buffer Overflow Vulnerability

Released May 05, 2000

Affects NetWin DNews 5.3

Reference **http://www.securityfocus.com/bid/1172**

Problem

- DNews News Server provides a CGI application that gives access to user’s NNTP server over the web. There are many unchecked buffers in the program, some of which can be exploited directly from any browser.
- Supplying an overlylong value for the "group", "cmd" and "utag" variables, and possibly others, will overwrite their respective buffers. In this manner, arbitrary code can be executed on the remote target.

SAFER

- Netwin has released patches which rectify this issue.

Gossamer Threads DBMan Information Leakage Vulnerability

Released May 05, 2000

Affects DBMan 2.0.4

Reference **http://www.securityfocus.com/bid/1178**

Problem

- Requesting an invalid database file from a web server implementing Gossamer Threads DBMan scripts will return a CGI error message containing environmental variables to a remote user without any authorization.
- The parameters displayed include the local document root path, server administrator account name, web server software, platform, etc.

SAFER

- Gossamer Threads has released the solution.

Aladdin Knowledge Systems eToken PIN Extraction Vulnerability

Released May 04, 2000

Affects Aladdin Knowledge Systems eToken 3.3.3x

Reference **http://www.securityfocus.com/bid/1170**

Problem

- Access to the eToken device itself and entering the PIN number encoded in the eToken will grant authorization to a local user. The PIN number can be reset to the default value with the use of standard device programmers. This can be done by physically opening the eToken device (which can be done without leaving any trace or evidence of tampering) and copying the default PIN value to the location used to store either the user PIN or administrator PIN in the serial EEPROM.

SAFER

- Vendor is working on a patch.

Netwin Dmailweb Server utoken Buffer Overflow Vulnerability

Released May 04, 2000

Affects NetWin DMail 2.5d

Reference **http://www.securityfocus.com/bid/1171**

Problem

- By providing a specially crafted, abnormally long "utoken" variable value it is possible to exploit an unchecked buffer and run arbitrary code on the Dmailweb server.

SAFER

- Netwin has release patches to rectify this issue.

Aladdin eToken 3.3.3.x Hardware USB Key Private Data Extraction

Released May 04, 2000

Affects Aladdin eToken USB Key 3.3.3.x

Reference **http://www.L0pht.com/**

Problem

- The attack requires physical access to the device circuit board and will allow all private information to be read from the device without knowing the PIN number of the legitimate user. By using any number of low-cost, industry-standard device programmers to modify the unprotected external memory, the User PIN can be changed back to a default PIN. This will allow the attacker to successfully login to the eToken and access all public and private data. A homebrew device programmer could be built for under $10 and commercial device programmers are available from a number of companies ranging in cost from $25 to $1000.
- Users must be aware that the PIN number can be bypassed and should not trust the security of the token if it is not always directly in their possession. If a legitimate user loses their USB key, all data, including the private information, needs to be considered to have been compromised.

SAFER

- Vendor is working on a patch.

Multiple Linux Vendor pam_console Vulnerability

Released May 03, 2000

Affects RedHat Linux 6.0 up to 6.2

Reference **http://www.securityfocus.com/bid/1176**

Problem

- pam_console exists to own certain devices to users logging in to the console of a Linux machine. It is designed to allow only console users to utilize things such as sound devices. It will chown devices to users upon logging in, and chown them back to being owned by root upon logout.
- However, as certain devices do not have a 'hangup' mechanism, like a tty device, it is possible for a local user to continue to monitor activity on certain devices after logging out. This could allow a malicious user to sniff other users console sessions, and potentially obtain the root password if the root user logs in, or a user su's to root. They could also surreptitiously execute commands as the user on the console.

SAFER

- Exploit code has been released for this problem. Patch should be released soon.

Multiple Vendor Predictable Resolver ID Vulnerability

Released May 03, 2000

Affects GNU glibc 2.0 up to2.1.3, ISC BIND 8.2 up to 8.2.2 p5

Reference **http://www.securityfocus.com/bid/1166**

Problem

- Vulnerability exists in the resolver routines supplied with glibc, up to and including 2.1.3. The glibc resolution routines will use information regarding the time on the machine, together with a process pid, to generate a random ID. Guessing this information intelligently is fairly easy. This, coupled with the fact that the resolver routines will discard any non-matching ID, allows for a brute force guess of the ID.
- The resolver library to match requests with queries uses ID’s. This is the only form of verification the host has that the return packets are actually from the nameserver it requested information from. Being able to predict this may make it possible to return bogus return information, or perform a variety of DNS based attacks.

SAFER

- The real world susceptibility of the resolver to the attacks above has not been demonstrated.

Cisco Router Online Help Vulnerability

Released May 03, 2000

Affects Cisco IOS, Cisco Router

Reference **http://www.securityfocus.com/bid/1161**

Problem

- Under certain revisions of IOS multiple Cisco routers have information leakage vulnerability in their online help systems. In essence this vulnerability allows users who currently have access to the router at a low level of privilege (users without access to the 'enable' password) can use the help system to view information which should only in theory be available to an 'enabled' user.
- This information is comprised of access lists among other things. The help system itself does not list these items as being available via the 'show' commands yet none the less it will execute them.

SAFER

- Cisco's Product Security Incident Response Team has confirmed the issue and approved the recommended workaround.

L-Soft Listserv 1.8 Web Archives Buffer Overflow Vulnerability

Released May 03, 2000

Affects L-Soft Listserv 1.8

Reference http://www.securityfocus.com/bid/1167

Problem

- The Web Archive component of L-Soft Listserv contains unchecked buffer code exploitable by sending specially crafted requests to the Web Archive.
- This weakness will allow execution of arbitrary code by remote attackers.

SAFER

- L-Soft has created an update to ListServ to address this issue.

UltraBoard Directory Traversal Vulnerability

Released May 03, 2000

Affects UltraScripts UltraBoard 1.6

Reference http://www.securityfocus.com/bid/1164

Problem

- UltraBoard 1.6 (and possibly all 1.x versions) is vulnerable to a directory traversal attack that will allow any remote browser to download any file that the webserver has read access to.
- On Windows installations, the file must reside on the same logical drive as the webroot. In all cases, the attacker must know the filename and relative path from the webroot.
- This is accomplished through a combination of the '../' string and the usage of a null byte (x00) in the variables passed to the UltraBoard CGI.

SAFER

- There is a new version of UltraBoard available (UltraBoard 2000) that may not be vulnerable in this manner. This is untested.

AppleShare IP 6.x Invalid Range Request Vulnerability

Released May 02, 2000

Affects Apple AppleShare IP 6.3, 6.2, 6.1

Reference http://www.securityfocus.com/bid/1162

Problem

- Requesting a URL with a specified range exceeding the physical limit of the file will cause the Web Server in AppleShare IP to return an extra 32 KB of information taken from RAM.
- The additional data will appear appended to the file requested and may contain sensitive information.

SAFER

- Apple Computer has released an upgrade which rectifies this issue.

Microsoft Windows 9x NetBIOS NULL Name Vulnerability

Released May 02, 2000

Affects Microsoft Windows 98, 95

Reference http://www.securityfocus.com/bid/1163

Problem

- Unpredictable results, including system crashes, lock-ups, reboots, and loss of network connectivity, can occur in Windows 95/98 if a NetBIOS session packet is received with the source host name set to NULL.

SAFER

- No patches have been released yet.

FileMaker Pro 5.0 Web Companion Software Multiple Vulnerabilities

Released May 02, 2000

Affects FileMaker FileMaker Pro 5.0

Reference **http://www.securityfocus.com/bid/1159**

Problem

- Web Companion Software is part of the Filemaker Pro 5.0 database package. Included in that package is the XML publishing capability, which does not make use of Filemaker Pro's web security features. Therefore any remote user can retrieve, via XML, any data from a web connected database regardless of the web security settings on that data.
- Filemaker Pro 5.0 also integrates email capabilities into web-based database applications. One of the features now available is the capability to specify contents of a database field for use as a format for an email. This feature bypasses Filemaker Pro's normal web security and allows any remote web user to send any database content to any email address regardless of the security settings for that content.
- The email features of Filemaker Pro also allow web users to anonymously forge emails.

SAFER

- FileMaker has released the patches which rectify this issue.

Sniffit '-L mail' Remote Buffer Overflow Vulnerability

Released May 02, 2000

Affects Brecht Claerhout Sniffit 0.3.7beta, 0.3.6HIP

Reference **http://www.securityfocus.com/bid/1158**

Problem

- Certain versions of the popular network sniffer package Sniffit have a buffer overflow which can be exploited remotely for root access. This buffer overflow in present in the code which handles sniffing mail headers.
- More specifically the overflow occurs when the logging flag '-L' contains the directive 'mail'.

SAFER

- Unofficial patch has been made available.

Cassandra NNTPServer v1.10 Buffer Overflow Vulnerability

Released May 1, 2000

Affects Atrium Software Cassandra NNTP Server 1.10

Reference **http://www.securityfocus.com/bid/1156**

Problem

- Unchecked buffer exists in the code that handles login information in Cassandra NNTP v1.10 server. Entering a login name that consists of over 10 000 characters will cause the server to stop responding until the administrator restarts the application.

SAFER

- It is not clear if the remote execution of code is possible. Updated version should be available shortly.

SECURITY ADVISORIES

This section contains official advisories as released by various vendors or security organizations. This list addresses the problems found during May 2000.

Red Hat Security Advisory 2000:005-05: New majordomo packages available

Released May 31, 2000

Affects Red Hat Powertools 6.1

Reference http://www.redhat.com/

Problem

- A vulnerability in /usr/lib/majordomo/resend and /usr/lib/majordomo/wrapper will allow execution of arbitrary commands with elevated privileges.

SAFER

- It is recommended that all users of Red Hat Linux using the majordomo package upgrade to the fixed package.

PGP Security Advisory: PGP 5.0 Vulnerabilities

Released May 30, 2000

Affects PGP 5.0 for Linux US Commercial, Freeware editions and Source code book

Reference http://www.nai.com/

Problem

- During a recent review of our published PGP 5.0 for Linux source code, researchers discovered that under specific, rare circumstances PGP 5.0 for Linux would generate weak, predictable public/private keypairs.
- Network Associates has verified that this issue does not exist in any other version of PGP.

SAFER

- Upgrade PGP to latest version.

Microsoft Security Bulletin (MS00-038)

Released May 30, 2000

Affects Microsoft Windows Media Encoder 4.0, 4.1

Reference http://www.microsoft.com/technet/security/bulletin/fq00-038.asp

Problem

- Windows Media Encoder is a component of the Windows Media Tools, which are part of the Windows Media Technologies. Windows Media Encoder is used to convert digital content into Windows Media Format for distribution by Windows Media Services in Windows NT and Windows 2000 Server. If a request with a particular malformation were sent to an affected encoder, it could cause it to fail, thereby denying formatted content to the Windows Media Server.
- This vulnerability would primarily affect streaming media providers that supply real-time broadcasts of streaming media - it would not prevent a Windows Media Server from distributing already-encoded data. The vulnerability cannot be used to cause a machine to crash, nor can it be used to usurp any administrative privileges. Simply locating the server could be a challenge, because the IP address of the Windows Media Encoder would typically not be advertised.

SAFER

- Microsoft has released a patch.

Microsoft Security Bulletin (MS00-035)

Released May 30, 2000

Affects Microsoft SQL Server 7.0 Service Packs 1 and 2

Reference **http://www.microsoft.com/technet/security/bulletin/fq00-035.asp**

Problem

- When SQL Server 7.0 Service Packs 1 or 2 are installed on a machine that is configured to perform authentication using Mixed Mode, the password for the SQL Server standard security System Administrator (sa) account is recorded in plaintext in the file \%TEMP%\sqlsp.log. The default permissions on the file would allow any user to read it who could log onto the server interactively.
- The password is only recorded if Mixed Mode is used, and even then, only if the administrator chose to use SQL Server Authentication when installing the service pack. Microsoft has long recommended that SQL servers be configured to use the more secure Windows NT Authentication Mode, and customers who have followed this recommendation would not be affected. Even on affected machines, the password could not be compromised if, per normal security recommendations, normal users are prevented from logging onto the machine interactively.

SAFER

- Microsoft has released a patch.

TurboLinux Security Announcement TLSA2000012-1: xlockmore-4.16 and earlier

Released May 29, 2000

Affects TurboLinux 6.0.4 and earlier

Reference **http://www.turbolinux.com/**

Problem

- The xlock program locks an X server until a valid password is entered. The command line option -mode provides a user with a mechanism to change the default display shown when the X server is locked. Xlock is installed with privileges to obtain password information, although these are dropped as early as possible.
- An overflow in the –mode command line option allows a malicious attacker to reveal arbitrary portions of xlock's address space including the shadow password file.

SAFER

- Update the package.

NAI Security Advisory COVERT-2000-06: Initialized Data Overflow in Xlock

Released May 29, 2000

Affects All versions of xlockmore prior to and including 4.16

Reference **http://www.nai.com/covert/**

Problem

- Implementation vulnerability in xlock allows global variables in the initialized data section of memory to be overwritten. This creates the potential for local users to view the contents of xlock's memory, including the shadowed password file, after root privileges have been dropped.

SAFER

- Patches and updates from various vendors are available.

SuSE Security Announcement: mufti

Released May 29, 2000

Affects SuSE Linux 6.1-6.4

Reference http://www.suse.com/

Problem

- The KDE CD player skid is setgid disk to be able to access the device file of the CDROM. To perform some action skid calls the unix command shell specified in the environment variable SHELL with the privileges of group disk.
- An adversary could set SHELL to his own program to get local root access to the system by writing directly to the raw HDD device.

SAFER

- Update the package.

NetBSD Security Advisory 2000-006: /etc/ftpchroot parsing broken in NetBSD-1.4.2

Released May 27, 2000

Affects NetBSD-1.4.2, NetBSD-current between 19990930 and 19991212

Reference http://www.netbsd.org/

Problem

- The chroot(2) system call, short for "change root", restricts a process to only be able to access a subtree of the filesystem.
- /etc/ftpchroot specifies users who are allowed to log in using ftp with a password, but are chroot'ed to their home directory, preventing them from accessing files outside their home directory via FTP. The incorrect fix in 1.4.2 caused the chroot call to not occur, allowing them regular, unprivileged access to files outside their home directory via FTP.

SAFER

- NetBSD has released patches for affected versions.

NetBSD Security Advisory 2000-005: Local "cpu-hog" denial of service

Released May 27, 2000

Affects NetBSD 1.4, 1.4.1, 1.4.2

Reference http://www.netbsd.org/

Problem

- 4.xBSD kernels are non-preemptive; processes running in user space can be preempted, but processes running in the kernel must yield the CPU voluntarily. Certain system calls could be convinced to run for an extended time in the kernel without yielding (e.g., reads from /dev/zero).
- In addition, the ktrace system-call tracing facility could use large amounts of kernel memory when tracing large I/O's

SAFER

- NetBSD has released patches for affected versions.

NetBSD Security Advisory 2000-004: SysV semaphore denial-of-service

Released May 27, 2000

Affects NetBSD 1.4, 1.4.1, 1.4.2

Reference http://www.netbsd.org/

Problem

- The undocumented semconfig(2) system call is used by ipcs(1) to "freeze" the state of semaphores so that a self-consistent snapshot could be displayed. However, this could then be abused to lock the semaphore system, preventing all semaphore operations from progressing, and leave it locked until the locking process exited.
- The fix is to disable this unnecessary locking; other comparable /dev/kmem-reading programs such as ps(1) and netstat(1) have never needed this sort of locking.
- Only programs that make use of semaphores are affected by this problem.

SAFER

- NetBSD has released patches for affected versions.

NetBSD Security Advisory 2000-003: Exploitable Vulnerability in Xlockmore

Released May 27, 2000

Affects NetBSD pkgsrc prior to 11th May 2000

Reference **http://www.netbsd.org/**

Problem

- The xlock program locks an X server until a valid password is entered. The command line option -mode provides a user with a mechanism to change the default display shown when the X server is locked. Xlock is installed with privileges to obtain password information, although these are dropped as early as possible.
- An overflow in the –mode command line option allows a malicious attacker to reveal arbitrary portions of xlock's address space including the shadow password file.

SAFER

- Upgrade xclockmore to version 4.16.1.

FreeBSD Security Advisory SA-00:20: krb5

Released May 26, 2000

Affects MIT Kerberos 5

Reference **http://www.freebsd.org/**

Problem

- The MIT Kerberos 5 port, versions 1.1.1 and earlier, contains several remote and local buffer overflows which can lead to root compromise. Note that the implementations of Kerberos shipped in the FreeBSD base system are separately-developed software to MIT Kerberos and are believed not to be vulnerable to these problems.
- However, a very old release of FreeBSD dating from 1997 (FreeBSD 2.2.5) did ship with a closely MIT-derived Kerberos implementation ("eBones") and may be vulnerable to attacks of the kind described here. Any users still using FreeBSD 2.2.5 and who have installed the optional Kerberos distribution are urged to upgrade to 2.2.8-STABLE or later. Note however that FreeBSD 2.x is no longer an officially supported version, nor are security fixes always provided.
- Local or remote users can obtain root access on the system running krb5.

SAFER

- Upgrade your entire ports collection and rebuild the krb5 port or download a new port skeleton for the krb5 port.

FreeBSD Security Advisory SA-00:19: semiconfig

Released May 26, 2000

Affects 386BSD-derived OSes, including all versions of FreeBSD, NetBSD and OpenBSD

Reference **http://www.freebsd.org/**

Problem

- An undocumented system call is incorrectly exported from the kernel without access-control checks. This operation causes the acquisition in the kernel of a global semaphore which causes all processes on the system to block during exit() handling, thereby preventing any process from exiting until the corresponding "unblock" system call is issued.
- This operation was intended for use only by ipcs(1) to atomically sample the state of System V IPC resources on the system (i.e., to ensure that resources are not allocated or deallocated during the process of sampling itself).
- An unprivileged local user can cause every process on the system to hang during exiting. In other words, after the system call is issued, no process on the system will be able to exit completely until another user issues the "unblock" call or the system is rebooted. This is a denial-of-service attack.

SAFER

- Upgrade to FreeBSD 2.1.7.1-STABLE, 2.2.8-STABLE, 3.4-STABLE, 4.0-STABLE or 5.0-CURRENT after the correction date.

TurboLinux Security Announcement TLSA2000011-1: gpm-1.19.1 and earlier

Released May 26, 2000

Affects TurboLinux 6.0.4 and earlier

Reference http://www.turbolinux.com/

Problem

- The gpm-root program, included in the gpm package, contains a programming error whereby a call to setgid() fails, and defaults to the group of the gpm-root binary. The group for the gpm-root binary in the affected installations is root.
- A user with console access can use this vulnerability to execute arbitrary commands with elevated privileges.

SAFER

- Update the packages.

CERT Advisory CA-2000-08: Inconsistent Warning Messages in Netscape Navigator

Released May 26, 2000

Affects Systems running Netscape Navigator, up to and including Navigator 4.73

Reference http://www.cert.org/

Problem

- A flaw exists in Netscape Navigator that could allow an attacker to masquerade as a legitimate web site if the attacker can compromise the validity of certain DNS information. This is different from the problem reported in CERT Advisory CA-2000-05, but it has a similar impact.
- If a user visits a web site in which the certificate name does not match the site name and proceeds with the connection despite the warning produced by Netscape, then subsequent connections to any sites that have the same certificate will not result in a warning message.

SAFER

- The CERT/CC recommends that prior to providing any sensitive information over SSL, you check the name recorded in the certificate to be sure that it matches the name of the site to which you think you are connecting.

NAI Security Advisory COVERT-2000-05: Microsoft Windows Computer Browser Reset

Released May 25, 2000

Affects All versions of Microsoft Windows 95, 98, NT and 2000

Reference http://www.nai.com/covert/

Problem

- The Microsoft Windows implementation of the Browser Protocol contains an undocumented feature that provides for the remote shutdown of the Computer Browser Service on a single computer or multiple computers.

SAFER

- Microsoft has released a patch for this vulnerability.

Cobalt Networks Security Advisory 5.25.2000

Released May 25, 2000

Affects Cobalt RaQ 3.0, 2.0

Reference http://www.cobaltnet.com/

Problem

- With the current installation of Frontpage on RaQ2 and RaQ3, the ability to write data to other websites hosted on the same RaQ. This is due to a permission issue with the 'httpd' user.

SAFER

- Cobalt Networks has produced a patch to correct this vulnerability.

Microsoft Security Bulletin (MS00-036)

Released May 25, 2000

Affects Microsoft Windows NT4.0, 2000

Reference **http://www.microsoft.com/technet/security/bulletin/fq00-036.asp**

Problem

- Windows NT 4.0 and Windows 2000 implement the CIFS Computer Browser protocol. Two vulnerabilities exist because of the inability of administrators to limit whether Master Browsers respond to certain frames.
- The ResetBrowser Frame vulnerability, which affects both Windows NT 4.0 and Windows 2000. Like most implementations, the Windows implementation provides the ability for a Master Browser to shut down other browsers via the ResetBrowser frame. However, there is no capability to configure a browser to ignore ResetBrowser frames. This could allow a malicious user to shut down browsers on his subnet as a denial of service attack against the browser service, or, in the worst case, to shut down all browsers and declare his machine the new Master Browser.
- The HostAnnouncement Flooding vulnerability, which does not affect Windows 2000. Because there is no means of limiting the size of the browse table in Windows NT 4.0, a malicious user could send a huge number of bogus HostAnnouncement frames to a Master Browser. The resulting replication traffic could consume most or all of the network bandwidth and cause other problems in processing the table as well.
- If a firewall were in place and blocking port 138 UDP, neither vulnerability could be exploited by an external user. Even an internal user could only attack browsers on the same subnet as his machine. Normal administrative tools would allow the administrator to determine who had mounted the attack.

SAFER

- Microsoft has released a patch.

CERT Advisory CA-2000-07: Microsoft Office 2000 UA ActiveX Control

Released May 24, 2000

Affects Systems with Internet Explorer and Microsoft Office 2000

Reference **http://www.cert.org/**

Problem

- The Microsoft Office 2000 UA ActiveX control is incorrectly marked as "safe for scripting". This vulnerability may allow an intruder to disable macro warnings in Office products and, subsequently, execute arbitrary code. This vulnerability may be exploited by viewing an HTML document via a web page, newsgroup posting, or email message.

SAFER

- Microsoft has produced a patch to correct this vulnerability.

Caldera Security Advisory CSSA-2000-013.0: buffer overflow in kdm

Released May 24, 2000

Affects OpenLinux Desktop 2.3, 2.4, OpenLinux eServer 2.3

Reference **http://www.calderasystems.com/**

Problem

- There is a buffer overflow in kdm, the KDE graphical login manager. Since the buffer variable that is affected is NOT on the stack but in the data area, it is not clear whether this bug can be exploited.

SAFER

- The proper solution is to upgrade to the fixed packages.

SGI Security Advisory 20000501-01-P: Vulnerability in infosrch.cgi

Released May 22, 2000

Affects IRIX 6.5-6.5.7

Reference http://www.sgi.com/

Problem

- The Infosearch(1) subsystem is used to search and browse virtually all SGI on-line documentation. The infosrch.cgi(1) is a program that allows access to infosearch(1) through a default installed HTTP web server on port 80.
- Unfortunately, vulnerability has been discovered in infosrch.cgi(1) which could allow any remote user to view files on the vulnerable system with privileges of the user "nobody".

SAFER

- Patches are available.

Microsoft Security Bulletin (MS00-029)

Released May 19, 2000

Affects Microsoft Windows 95, 98, NT4.0, 2000

Reference http://www.microsoft.com/technet/security/bulletin/fq00-029.asp

Problem

- The affected systems contain a flaw in the code that performs IP fragment reassembly. If a continuous stream of fragmented IP datagrams with a particular malformation were sent to an affected machine, it could be made to devote most or all of its CPU availability to processing them. The data rate needed to completely deny service varies depending on the machine and network conditions, but in most cases even relatively moderate rates would suffice.
- The vulnerability would not allow a malicious user to compromise data on the machine or usurp administrative control over it. Although it has been reported that the attack in some cases will cause an affected machine to crash, affected machines in all Microsoft testing returned to normal service shortly after the fragments stopped arriving. Machines protected by a proxy server or a firewall that drops fragmented packets would not be affected by this vulnerability. The machines most likely to be affected by this vulnerability would be machines located on the edge of a network such as web servers or proxy servers.

SAFER

- Microsoft has released a patch.

IBM Security Advisory ERS-OAR-E01-2000:087.1

Released May 19, 2000

Affects IBM AIX versions 3.2.x, 4.1.x, 4.2.x, 4.3.x

Reference http://techsupport.services.ibm.com/

Problem

- Local users could gain write access to some files on local or remotely mounted AIX filesystems, even though the file permissions do not allow write access. This vulnerability was discovered in the IBM laboratory during analysis of filesystem behavior and is not exposed during normal system operation.
- A local user could gain write access to some files on local or remotely mounted AIX filesystems, even though the file permissions do not allow write access.

SAFER

- IBM has released patches.

RatHat Security Advisory-2000:028-02: Netscape 4.73 available

Released May 19, 2000

Affects Netscape Communicator 4.05 up to 4.72

Reference **http://www.redhat.com/**

Problem

- Vulnerability exists in the manner in which versions of Netscape Communicator up to, but not including, 4.73, validate SSL certificates. This vulnerability could make it possible for the integrity of an SSL connection to be compromised.

SAFER

- Upgrading to Netscape Communicator 4.73 will solve this problem.

Caldera Security Advisory CSSA-2000-011.0: several problems in xemacs

Released May 18, 2000

Affects OpenLinux Desktop 2.3, 2.4, OpenLinux eServer 2.3

Reference **http://www.calderasystems.com/**

Problem

- Under some circumstances, users are able to snoop on other users' keystrokes. This is a serious problem if you use modules that require e.g. input of passwords, such as MailCrypt.
- Temporary files are created insecurely.

SAFER

- The proper solution is to upgrade to the fixed packages.

SuSE Security Announcement: kernel

Released May 17, 2000

Affects SuSE Linux 6.1up to 6.4

Reference **http://www.suse.com/**

Problem

- The masquerading feature in the Linux kernel has got vulnerability in the udp and ftp masquerading code which allows arbitrary backward connections to be opened. Some denials of service were found.
- Remote users may bypass ipchains filter rules protecting the internal network. Users can crash the machine.

SAFER

- SuSE released update.

Microsoft Security Bulletin (MS00-033)

Released May 17, 2000

Affects Microsoft Internet Explorer 4.0, 4.01, 5.0, 5.01

Reference **http://www.microsoft.com/technet/security/bulletin/fq00-033.asp**

Problem

- The bulletin is related with three security vulnerabilities unrelated to each other except by the fact that they all occur in the same .dll.
- "Frame Domain Verification" vulnerability. When a web server opens a frame within a window, the IE security model should only allow the parent window to access the data in the frame if they are in the same domain. However, two functions available in IE do not properly perform domain checking, with the result that the parent window could open a frame that contains a file on the local computer, then read it. This could allow a malicious web site operator to view files on the computer of a visiting user. The web site operator would need to know (or guess) the name and location of the file, and could only view file types that can be opened in a browser window.
- "Unauthorized Cookie Access" vulnerability. By design, the IE security model restricts cookies so that they can be read only by sites within the originator's domain. However, by using an especially malformed URL, it is possible for a malicious web site operator to gain access to another site's cookie and read, add or change them. A malicious web site operator would need to entice a visiting user into clicking a link in order to access each cookie, and could not obtain a listing of the cookies available on the visitor's system. Even after recovering a cookie, the type and amount of personal information would depend on the privacy practices followed by the site that placed it there.
- "Malformed Component Attribute" vulnerability. The code used to invoke ActiveX components in IE has an unchecked buffer and could be exploited by a malicious web site operator to run code on the computer of a visiting user. The unchecked buffer is only exposed when certain attributes are specified in conjunction with each other.

SAFER

- The patch also eliminates a new variant of the previously addressed WPAD Spoofing vulnerability.

FreeBSD Security Advisory SA-00:08 revised: Lynx ports contain numerous buffer overflows

Released May 17, 2000

Affects lynx prior to version 2.8.3pre.5

Reference **http://www.freebsd.org/**

Problem

- Versions of the lynx software prior to version 2.8.3pre.5 were written in a very insecure style and contain numerous potential and several proven security vulnerabilities (publicized on the BugTraq mailing list) exploitable by a malicious server.
- A malicious server that is visited by a user with the lynx browser can exploit the browser security holes in order to execute arbitrary code as the local user.

SAFER

- Upgrade to lynx or lynx-current after the correction date.

TurboLinux Security Announcement TLSA2000010-1: OpenLDAP 1.2.9 and earlier

Released May 17, 2000

Affects TurboLinux 6.0.2 and earlier

Reference **http://www.turbolinux.com/**

Problem

- OpenLDAP follows symbolic links when creating files. The default location for these files is /usr/tmp, which is a symlink to /tmp, which in turn is a world-writable directory.
- Local users can destroy the contents of any file on any mounted filesystem.

SAFER

- Update the packages.

CERT Advisory CA-2000-06: Multiple Buffer Overflows in Kerberos Authenticated Services

Released	May 17, 2000
Affects	Systems running Kerberos 4/5
Reference	http://www.cert.org/

Problem

- Serious buffer overrun vulnerabilities exist in many implementations of Kerberos 4, including implementations included for backwards compatibility in Kerberos 5 implementations. Other less serious buffer overrun vulnerabilities have also been discovered. ALL KNOWN KERBEROS 4 IMPLEMENTATIONS derived from MIT sources are believed to be vulnerable.

SAFER

- Various patches and workaround are available.

HP Security Advisory #00114: Sec. Vulnerability in BIND

Released	May 17, 2000
Affects	HP9000 Series 700/800 running HP-UX releases 10.XX & 11.XX
Reference	http://us-support.external.hp.com/

Problem

- The CERT advisory (CA-99-14) detailed several BIND vulnerabilities. The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols.
- This vulnerability may allow remote users to gain root access or to disrupt normal operation on the name server.

SAFER

- Install patches that upgrade BIND to version 4.9.7, or upgrade to version 8.1.2.

Cisco Security Advisory: Cisco IOS HTTP Server Vulnerability

Released	May 14, 2000
Affects	Different versions of Cisco Routers, switches etc …
Reference	http://www.cisco.com/

Problem

- A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled and browsing to "http://<router-ip>/%%" is attempted. This defect can be exploited to produce a denial of service (DoS) attack. This defect has been discussed on public mailing lists and should be considered public information.
- The vulnerability, identified as Cisco bug ID CSCdr36952, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 11.1 through 12.1, inclusive.

SAFER

- Cisco has released patches for vulnerability.

CERT Advisory CA-2000-05: Netscape Navigator Improperly Validates SSL Sessions

Released	May 12, 2000
Affects	Netscape Navigator 4.72, 4.61, 4.07, probably other versions too
Reference	http://www.cert.org/

Problem

- Netscape Navigator correctly checks the certificate conditions (*) at the beginning of a SSL session it establishes with a certain web server. The flaw is, while this SSL session is still alive, all HTTPS connections to *THAT SERVER'S IP ADDRESS* are assumed to be a part of this session (and therefore certificate conditions are not checked again).
- Instead of comparing hostnames to those of currently open sessions, Navigator compares IP addresses. Since more than one hostname can have the same IP address, there is a great potential for security breach. This behavior is not in compliance with SSL specification.

SAFER

- Netscape has (even prior to our notification - see the Acknowledgments section) provided a Navigator Add-on called Personal Security Manager (PSM).

Microsoft Security Bulletin (MS00-034)

Released May 12, 2000

Affects Microsoft Office 2000

Reference **http://www.microsoft.com/technet/security/bulletin/fq00-034.asp**

Problem

- An ActiveX control that ships as part of Office 2000 is incorrectly marked as "safe for scripting". This control, the Office 2000 UA Control, is used by the "Show Me" function in Office Help, and allows Office functions to be scripted. A malicious web site operator could use the control to carry out Office functions on the machine of a user who visited his site.
- The control ships only as part of Office 2000 (and Office 2000 family members, as listed below). The patch removes all unsafe functionality, with the result that the "Show Me" function will be disabled in Office 2000.

SAFER

- Microsoft has released a patch.

Microsoft Security Bulletin (MS00-030)

Released May 11, 2000

Affects Microsoft Internet Information Server 4.0, 5.0

Reference **http://www.microsoft.com/technet/security/bulletin/fq00-030.asp**

Problem

- In compliance with RFC 2396, the algorithm in IIS that processes URLs has flexibility built in to allow it to process any arbitrary sequence of file extensions or subresource identifiers (referred to in the RFC as path_segments). By providing an URL that contains especially malformed file extension information, a malicious user could misuse this flexibility in order to arbitrarily increase the work factor associated with parsing the URL. This could consume much or all of the CPU availability on the server and prevent useful work from being done.
- The vulnerability does not provide any capability to cause the server to fail, or to add, change or delete data on it. Likewise, it provides no capability to usurp administrative control of the web server. The slowdown would only last until the URL had been processed, at which point service would return to normal.

SAFER

- Microsoft has released a patch.

ISS Security Advisory: Microsoft IIS Remote Denial of Service Attack

Released May 11, 2000

Affects Microsoft IIS 4.0 and 5.0

Reference **http://www.iss.net/**

Problem

- The vulnerability exists primarily in IIS 4.0 and to a limited extent in 5.0. IIS uses IISADMPWD virtual directory to give users the ability to change passwords. When IIS is installed, it creates the directory %system32%\inetsrv\iisadmpwd that contains .htr files used for web-based password administration. Only when the virtual directory IISADMPWD is created does the ability to change passwords become enabled.
- On vulnerable systems, an attacker can send a malformed request to force inetinfo.exe to utilize 100% of the CPU and adversely affect the ability of IIS to field requests. After the vulnerability has been exploited, the inetinfo.exe process cannot be stopped, requiring a full reboot of the server to regain functionality. The effect on IIS 5.0 is not as severe. If the vulnerability is exploited against this version of IIS, access to any .htr file on the server fails. CPU utilization does not increase to 100% as it does in version 4.0.

SAFER

- Microsoft has made patches available for IIS versions 4 and 5.

Microsoft Security Bulletin (MS00-031)

Released May 10, 2000

Affects Microsoft IIS 4.0 and 5.0

Reference **http://www.microsoft.com/technet/security/bulletin/fq00-031.asp**

Problem

- The bulletin is related with two security vulnerabilities that are unrelated except by virtue of the fact that both exist in the ISAPI extension that provides web-based password administration via .HTR scripts.
- The "Undelimited .HTR Request" vulnerability is a denial of service vulnerability. If a malicious user provided a password change request that was missing an expected delimiter, the algorithm would conduct an unbounded search. This would prevent it from servicing additional .HTR requests, and could also slow the overall response of the server.
- The ".HTR File Fragment Reading" vulnerability could allow fragments of certain types of files to be read by providing a malformed request that would cause the .HTR processing to be applied to them. However, the vulnerability could only be exploited under extremely restrictive conditions, and the most valuable data in the files would be the least likely to actually appear in the fragments sent to the user.
- Neither of these vulnerabilities would allow data to be added, deleted or changed on the server, nor would they allow any administrative control on the server to be usurped. Although .HTR files are used to allow web-based password administration, neither of these vulnerabilities involves any weakness in password handling. Also, if security best practices have been followed, and unneeded script mappings have been removed, many customers will have removed the .HTR script mapping and thus be unaffected by either vulnerability.

SAFER

- Microsoft has released a patch.

FreeBSD Security Advisory SA-00:17: Buffer overflow in libmytinfo

Released May 09, 2000

Affects FreeBSD 3.x

Reference **http://www.freebsd.org/**

Problem

- libmytinfo allows users to specify an alternate termcap file or entry via the TERMCAP environment variable, however this is not handled securely and contains an overflowable buffer inside the library. This is security vulnerability for binaries which are linked against libmytinfo and which are setuid or setgid (i.e. run with elevated privileges). It may also be vulnerability in other more obscure situations where a user can exert control over the environment with which another user runs an ncurses binary.
- FreeBSD 3.x and earlier versions use a very old, customized version of ncurses which is difficult to update without breaking backwards-compatibility. The update was made for FreeBSD 4.0, but it is unlikely that 3.x will be updated. However, the ncurses source is currently being audited for further vulnerabilities.
- Certain setuid/setgid third-party software (including FreeBSD ports/packages) may be vulnerable to a local exploit yielding privileged resources, such as network sockets, privileged filesystem access, or outright privileged shell access (including root access).

SAFER

- Remove any setuid or setgid binary which is linked against libmytinfo (including statically linked), or remove set[ug]id privileges from the file as appropriate.

Allaire Security Bulletin (ASB00-12): Allaire ClusterCATS URL Redirect Vulnerability

Released May 08, 2000

Affects Allaire ClusterCATS 1.0

Reference **http://www.allaire.com/**

Problem

- While performing a URL redirect, Allaire ClusterCATS may append stale information to the URL that can contain sensitive information.

SAFER

- Allaire has released a patch, which rectifies this issue.

NetBSD Security Advisory 2000-002: IP options processing Denial of Service

Released May 07, 2000

Affects NetBSD 1.4 up to 1.4.2 Alpha and SPARC

Reference http://www.netbsd.org/

Problem

- Vulnerability exists in the 1.4.x NetBSD kernel that may allow remote attackers to cause the machine to kernel panic on certain architectures. By sending a packet to a machine running the Alpha or SPARC versions of NetBSD, with an unaligned IP timestamp option, it is possible to cause the kernel to perform an unaligned memory access. This will cause a panic, causing the machine to reboot.
- x86 and arm32 platforms have a similar bug. However, as both of these architectures can perform unaligned memory accesses, this vulnerability does not cause them to panic.

SAFER

- Patches are available from NetBSD.

FreeBSD Security Advisory SA-00:18: gnapster port allows remote users to view local files

Released May 05, 2000

Affects Knapster 0.9, Gnapster 1.3.8

Reference http://www.freebsd.com/

Problem

- Various open source clones of the Napster software package have a vulnerability by which users may view files on a machine running a vulnerable Napster clone client.
- The file access is limited to files accessible by the user running the client. The official commercial version of Napster does not contain this vulnerability.

SAFER

- Upgrades for FreeBSD ports, and source patches, are available.

FreeBSD Security Advisory SA-00:16: golddig port allows users to overwrite local files

Released May 05, 2000

Affects Alexander Siegel golddig 2.0

Reference http://www.freebsd.com/

Problem

- It was discovered during a security audit of the golddig2 package by the FreeBSD ports team, that the makelev program can be used to overwrite arbitrary files, as it is by default installed setuid root.
- The content of the file is not arbitrary, however, so it is not immediately clear whether this program could be used to elevate privilege. That the makelev program being setuid is a potential security problem is documented in the original Makefile for golddig.

SAFER

- FreeBSD has issued updated ports packages.

HP Security Advisory #00113: Sec. Vulnerability with shutdown command

Released May 04, 2000

Affects HP-UX 11.0, 10.20, 10.10, HP VirtualVault 11.4, 10.24

Reference http://us-support.external.hp.com/

Problem

- Vulnerability exists in the 'shutdown' program, as included with versions 10 and 11 of HP-UX, and HP-UX VirtualVault (VVOS), from Hewlett Packard.
- The exact nature of this vulnerability was not made available. From the wording of the advisory, it appears to be a buffer overflow.

SAFER

- Patches are available from HP.

NAI Security Advisory-May042000: Trend Micro InterScan VirusWall Remote Overflow

Released May 04, 2000

Affects Trend Micro InterScan VirusWall 3.0.1 up to 3.32

Reference http://www.nai.com/covert/

Problem

- InterScan VirusWall includes the ability to scan for virii in uuencoded files. Due to an unchecked buffer in the code, if a uuencoded file is sent that includes an embedded final filename of more than 128 characters, arbitrary remote code can be executed at the privilege level of the VirusWall software.
- In an NT installation, VirusWall runs as SYSTEM by default.

SAFER

- Trend Micro has rectified this issue with the release of InterScan VirusWall 3.4 Beta and a patch.

ISS Security Advisory: Vulnerability in Quake3Arena Auto-Download Feature

Released May 03, 2000

Affects ID Software Quake3 Arena 1.16n

Reference http://www.iss.net/

Problem

- The Quake3Arena game is vulnerable to a directory traversal attack when participating in games hosted on remote servers.
- A Quake3 Arena server is capable of gaining read or writes access and executing arbitrary code on machines connecting to their server participating in a multi-player game. The Quake3 Arena server operator can access and write to any known directory above the subdirectory of the Quake3 Arena install directory. This is due to the implementation of the Software Developers Kit (SDK) shipped with Quake3 Arena which allows for modifications to the filesystem, and the failure of the client to properly handle the '..\' string.
- Attempting to access files above the subdirectory of the install directory will display an error message, however, access is still granted. This vulnerability in conjunction with the Automatic Download feature in Quake3 Arena can be used to launch an attack.

SAFER

- Select the 'setup' option from the main menu and choose 'game options.' From there, disable the 'automatic downloading' feature.

SuSE Security Announcement: aaa_base

Released May 02, 2000

Affects All versions of SuSE Linux

Reference http://www.suse.com/

Problem

- aaa_base is the basic package that comes with any SuSE Linux installation. Two vulnerabilities have been found.
- The cron job /etc/cron.daily/aaa_base does a daily checking of files in /tmp and /var/tmp, where old files will be deleted if configured to do so. Please note this this feature is NOT activated by default. If the /tmp cleanup is activated, any file or directory can be deleted by any local user
- Some system accounts have their home directories set to /tmp by default. These are the users games, firewall, wwwrun and nobody on a SuSE 6.4. If an attacker creates dot files in /tmp (e.g. bash profiles), these might be executed if someone uses e.g. "su - nobody" to switch to the nobody user. This can lead to a compromise of that userid. This vulnerability is present in several other unix systems as well - please check all!

SAFER

- Update the package.

HP Security Advisory #00104 revised: Sec. Vulnerability regarding automountd (rev. 01)

Released	May 02, 2000
Affects	HP-9000 Series 700/800 HP-UX releases 10.20 and 11.00
Reference	**http://us-support.external.hp.com/**

Problem

- This problem was originally reported in CERT Advisory CA-99-05, regarding the vulnerability in automountd, which allows an intruder to execute arbitrary commands with the privileges of the automountd process.
- We had previously reported that Hewlett-Packard platforms were not vulnerable; we now have new information showing that we are indeed vulnerable.

SAFER

- Patches for this vulnerability are now available from HP.

DENIAL-OF-SERVICE

Denial-of-Service attacks are becoming an increasing concern. Below is a compilation of denial-of-service security problems found in May 2000.

Cerberus Information Security Advisory (CISADV000527): Windows NT Browser Service DoS

Released May 30, 2000

Affects Microsoft Windows NT 4.0

Reference **http://www.cerberus-infosec.co.uk/advisories.html**

Problem

- A serious security flaw exists within the Computer Broswer Service on Windows NT 4 that can lead to a total network failure due to bandwidth starvation.
- Remote attacker could flood Master Browser with 'host announcement' messages, and cause the list to be broadcasted to all other stations on the network, causing overload on the network.

SAFER

- Microsoft have issued a patch.

Deerfield MDaemon Mail Server DoS Vulnerability

Released May 24, 2000

Affects Mdaemon 3.1beta, 3.0.3

Reference **http://www.securityfocus.com/bid/1250**

Problem

- Entering a long argument to the user command (256 or more bytes) will overflow the user buffer and will cause the Mdaemon mail server to stop responding after the pass command is issued. A reboot is required in order to regain normal functionality.

SAFER

- Deerfield.com is aware of this vulnerability and will be addressing this issue in the next release of 3.1 beta.

HP Web JetAdmin 6.0 Printing DoS Vulnerability

Released May 24, 2000

Affects HP JetAdmin 6.0

Reference **http://www.securityfocus.com/bid/1246**

Problem

- By default JetAdmin Web Interface Server listens on port 8000. If a malformed URL request is sent to port 8000 this will cause the server services to stop responding. The service must be stopped and restarted to regain normal functionality.

SAFER

-

TopLayer AppSwitch 2500 Multiple DoS Vulnerabilities

Released May 20, 2000

Affects TopLayer AppSwitch 2500.0

Reference **http://www.securityfocus.com/bid/1258**

Problem

- TopLayer AppSwitch 2500 has been reported to be vulnerable to numerous DoS attacks. Fragmented packets, bad ICMP checksums, and other anomalous packets are reported to crash the switch.

SAFER

- Wait for official fix, or use some other switch.

Nite Server FTPd Multiple DoS Vulnerabilities

Released May 19, 2000

Affects Nite Server 1.7, 1.6, 1.5

Reference **http://www.securityfocus.com/bid/1230**

Problem

- Multiple denials of service vulnerabilities exist in Nite Server FTP daemon.
- Requesting an unusually long string of characters in the user command will cause the daemon to utilize all available memory, leaving the server to hang.
- If a remote user enters endless characters in the password field without ever terminating the request, the daemon allocates all available memory and denies any new connections
- By logging on and making a request, which consists of malformed data and immediately logging off, the ftp server will deny any new connections.
- When renaming files, if the new filename provided is too long, the server will stop accepting new connections.

SAFER

- Updated version will be available shortly.

Microsoft Windows 9x / NT 4.0 / 2000 Fragmented IP Packets DoS Vulnerability

Released May 19, 2000

Affects Microsoft Windows 95, 98, NT4.0, 2000

Reference **http://www.securityfocus.com/bid/1236**

Problem

- Transmitting identical fragmented IP Packets to a Windows 9x, NT 4.0, NT Terminal Server, or 2000 host at a rate of approximately 150 packets per second will cause the target's CPU utilization to reach 100%. CPU utilization will return to normal after the attack has ceased. In some cases, this attack could produce a blue screen of death.
- The DoS initiated by this attack may not be related to IP fragmentation but rather to resource exhaustion and a problem in filtering bad packets by Microsoft Windows.

SAFER

- Microsoft has released the patches that rectify the issue.

Axent NetProwler Malformed IP Packets DoS Vulnerability

Released May 18, 2000

Affects Axent NetProwler 3.0

Reference **http://www.securityfocus.com/bid/1225**

Problem

- Axent NetProwler 3.0 IDS is vulnerable to a malformed packet attack. It will crash if the Man-in-the-Middle signature encounters a packet for which the following expression is true: (IP_HEADER_LENGTH + TCP_HEADER_LENGTH) > IP_TOTAL_LENGTH
- In addition, NetProwler utilizes Microsoft JET engine 3.5 for storing incoming alert information.

SAFER

- In NetProwler 3.0, disable the Man-in-the-Middle signature for all monitored hosts.

XFree86 Xserver Denial of Service Vulnerability

Released May 18, 2000

Affects XFree86 X11R6 4.0, 3.3.6, 3.3.5

Reference http://www.securityfocus.com/bid/1235

Problem

- A remote user can send a malformed packet to the TCP listening port, 6000, which will cause the X server to be unresponsive for some period of time. During this time, the keyboard will not respond to user input, and in some cases, the mouse will also not respond.
- During this time period, the X server will utilize 100% of the CPU, and can only be repaired by being signaled. This vulnerability exists only in servers compiled with the XCSECURITY #define set. This can be verified by running the following: strings /path/to/XF86_SVGA | grep "XC-QUERY-SECURITY-1"

SAFER

- Run the X server with the option "-nolisten tcp" set. This option causes the X server to not listen connections from any client. To use this option, simply add it to serverargs variable in the /usr/X11/bin/startx script.

BeOS TCP Fragmentation Remote DoS Vulnerability

Released May 18, 2000

Affects BeOS 5.0

Reference http://www.securityfocus.com/bid/1222

Problem

- BeOS is vulnerable to a remote TCP fragmentation attack that will crash the target system, requiring a reboot.

SAFER

- New version of BeOS should have the whole TCP/IP stack rewritten. Until then, users will have to remain vulnerable, since BE did not provide any patches for this problem.

Cayman 3220-H DSL Router DoS Vulnerability

Released May 17, 2000

Affects Cayman 3220-H DSL Router 1.0, Cayman GatorSurf 5.5 Build R0, 5.3 build R1, R2

Reference http://www.securityfocus.com/bid/1219

Problem

- Large usernames or passwords sent to the router's HTTP interface restart the router. Router log will show "restart not in response to admin command"

SAFER

- Upgrading to GatorSurf software version 5.5.0 Build R1 will solve this issue.

CProxy 3.3 SP2 Buffer Overflow DoS Vulnerability

Released May 16, 2000

Affects CProxy Server 3.3SP2

Reference http://www.securityfocus.com/bid/1213

Problem

- A buffer overflow DoS vulnerability exists in CProxy Server 3.3 Service Pack 2.

SAFER

- New version has been made available. Upgrade.

Allaire ColdFusion 4.5.1 Cached File Request DoS Vulnerability

Released May 10, 2000

Affects Allaire ColdFusion Server 4.5.1

Reference **http://www.securityfocus.com/bid/1192**

Problem

- It is possible to remotely halt the operation of Allaire ColdFusion Server by requesting a cached file that is no longer stored in memory and contains a <CFCACHE> tag. Other conditions that are necessary in order to reliably cause a denial of service in this instance are that there are no running thread request slots available at the time of the cached file request, knowledge of the timeout period, last cached date/time, and 'Limit Simultaneous Requests' setting (which is by default, 5), and the use of a load generator or DoS tool.
- Most of these requirements can be met by performing various reconnaissance actions against the server, or ignored by making relatively safe assumptions, taking into account the default settings and the traffic levels/popularity of the server.
- The default number of cached file requests that ColdFusion Server can handle is 5. Therefore, 6 simultaneous requests for the same cached file no longer in memory could possibly cause the server to stop responding and will require to be restarted in order to regain normal functionality.

SAFER

- Allaire released patches on January 4, 2000 regarding potential information leakage by the CFCACHE tag, which will also clear up this vulnerability.

UltraBoard DoS Vulnerability

Released May 05, 2000

Affects UltraScripts UltraBoard 1.6

Reference **http://www.securityfocus.com/bid/1175**

Problem

- UltraBoard 1.6 (and possibly all 1.x versions and the new beta Ultraboard 2000) are vulnerable to this Denial of Service attack.
- A remote user is able to expend all of the available resources of the webserver by using a specially devised request to the CGI. This request causes a fork, which will then consume the processor time and memory of the server.

SAFER

- Typical resource exhaustion attack.

Linux knfsd Denial of Service Vulnerability

Released May 01, 2000

Affects Linux kernel 2.3.x, 2.2.x, 2.1.x

Reference **http://www.securityfocus.com/bid/1160**

Problem

- Due to inconsistencies in differentiating between signed and unsigned integers within the program, it becomes possible for a remote, unauthenticated user to cause the knfsd, and NFS service, to be unavailable.

SAFER

- Upgrading to the latest versions of the 2.2.x (2.2.15-pre20) or 2.2.3 (2.3.99-pre7) kernel will remedy this problem.

SECURITY BUGS

Many security problems are too specific to become a full advisory. Below is a list of security problems discovered in various softwares during the month of May 2000, which we advise you to check against your IT environment.

Remote Dos attack against Intel express 8100 router

Intel express 8100 isdn router vulnerable for remote icmp fragmented packets and oversize packets. Download libnet and isic-0.05 test following exploit. And do the following command to generate oversized and fragmented packets: ./icmpsic -s 127.0.0.1,23 -d <target.router.ip.address> -F 100. After a couple of minutes router hangs. No patch from the vendor yet.

Allmanage.pl vulnerability

Websites using 'Allmanage Website Administration Software 2.6 WITH the upload ability', and maybe earlier versions, contain a vulnerability which gives you full add/del/change access in the user-account directories and you can change the files in the main directory of the CGI script. Go instead of /allmanage.pl to /allmanageup.pl (extension can be .cgi eventually). You'll get into the "Upload Successful! page" and press on the 'Return To Filemanager'-button. Now you'll get into the Root Directory. From here you can add, change, delete user-accounts and change the contents of the directory main page. This vulnerability is only tested with the Perl version of the script on 9 different sites, all were vulnerable, and it is not tested with the MySQL version and earlier releases.

Allmanage.pl Admin Password vulnerability

Everybody can easily get the admin password from the allmanage directory. You are able to set/change lots of variables, add accounts, mail users, backup, restore, edit header/footer code etc… Find were allmanage.pl is located and change allmanage.pl with K. For example: allmanage/allmanage.pl will become allmanage/k. This file contains the admin password, not encrypted. Go to allmanage_admin.pl instead of allmanage.pl and login. You can use admin as loginname. Now you're in the main admin panel. N.B. loginname is not always admin, but in most of the cases it is. That is tried on 8 sites using allmanage.pl. 6 of them were vulnerable. Other interesting files to request: adp : Admin information and encrypted password userfile.dat: All user information they entered requesting their account. (N.B. not always there) settings.cfg: Config file, you can get the same information out of the admin panel. This may also work on the version without the upload ability.

PC-Cillin vulnerability

Version 6.x of Trend Micro's PC-Cillin Anti-Virus software can be a subject to a remote DoS attack and possibly unauthorized relays. As part of its Java/ActiveX protection, it routes all http requests through its own internal proxy on port 8431. Unfortunately, it allows anyone anywhere to connect to that port and dump enough data through it to saturate an unexpected victims connection. Trend’s Micro technical support could not confirm or deny if remote users are able to get an outbound connection from the victims system.

UNDERGROUND TOOLS

Here are the new tools that hackers/crackers will soon use against your systems. We do not recommend that you use such tools against any resources without prior authorization. We only list new tools published since the last issue of SAFER.

SCANNERS

nmap-2.54BETA1.tar.gz
New, very cool, option –sO has been added (scan for protocols).

magdalena.pl
Small utility written in perl that will scan a list of hostnames for a certain CGI.

twwwscan.exe
Windows based WWW vulnerability scanner.

sara-3.0.5.tar.gz
Security audit tool based on SATAN.

ucgi240.c
CGI vulnerability scanner.

EXPLOITS

sniffit.c
Exploit for Sniffit '-L mail' Remote Buffer Overflow Vulnerability

5niffi7.c
Exploit for Sniffit '-L mail' Remote Buffer Overflow Vulnerability

RFParalyze.c
Exploit for Microsoft Windows 9x NetBIOS NULL Name Vulnerability

listservbo.c
Exploit for L-Soft Listserv 1.8 Web Archives Buffer Overflow Vulnerability

pam_console.c
Exploit for Multiple Linux Vendor pam_console Vulnerability

heimlich.zip
Exploit for Aladdin Knowledge Systems eToken PIN Extraction Vulnerability

ADMDNews.zip
Exploit for Netwin DNews News Server Buffer Overflow Vulnerability

ipivot.tar.gz
Exploit for NetStructure 7110 Undocumented Password Vulnerability

gnapster-exp.pl
Exploit for Gnapster and Knapster File Access Vulnerability

bugzilla-exp.pl
Exploit for Bugzilla 2.8 Unchecked Existing Bug Report Vulnerability

netprex-sparc.c
Exploit for Solaris netpr Buffer Overflow Vulnerability

netprex-x86.c
Exploit for Solaris netpr Buffer Overflow Vulnerability

dnslong.c
Exploit for AntiSniff DNS Overflow Vulnerability

lo.c
Exploit for AntiSniff DNS Overflow Vulnerability

antisniffexpl2.c
Exploit for AntiSniff DNS Overflow Vulnerability

klogin-bsdi.c
Exploit for Multiple Vendor Kerberos 5/ 4 Compatibility krb_rd_req() Buffer Overflow Vulnerability

ksux.c
Exploit for Multiple Vendor Kerberos 5/ 4 Compatibility krb_rd_req() Buffer Overflow Vulnerability

kshux.c
Exploit for Multiple Vendor Kerberos 5/ 4 Compatibility krb_rd_req() Buffer Overflow Vulnerability

7350kscd.tgz
Exploit for KDE kscd SHELL Environmental Variable Vulnerability

RFPickaxe.pl
Exploit for NetworkICE ICECap Manager Default Username and Password Vulnerability

xsoldier.c
Exploit for FreeBSD and Linux Mandrake 'xsoldier' Buffer Overflow Vulnerability

xsol-x.c
Exploit for FreeBSD and Linux Mandrake 'xsoldier' Buffer Overflow Vulnerability

smtpkill.pl
Exploit for Lotus Domino Server ESMTP Buffer Overflow Vulnerability

animal.c
Exploit for Gauntlet Firewall Remote Buffer Overflow Vulnerability

fd-ex.c
Exploit for Multiple Linux Vendor fdmount Buffer Overflow Vulnerability

fdmnt-smash2.c
Exploit for Multiple Linux Vendor fdmount Buffer Overflow Vulnerability

breakgdm.c
Exploit for GNOME gdm XDMCP Buffer Overflow Vulnerability

qpop_euidl.c
Exploit for Qualcomm Qpopper 'EUIDL' Format String Input Vulnerability

ksux.c
Exploit for Kerberos ksu

kshux.c
Exploit for Kerberos krshd

l0phtl0phe.c
antisniff x86/linux remote root exploit

kdesud-xpl.c
Exploit for KDE kdesud DISPLAY Environment Variable Overflow

cdburner-exp.c
Exploit for Linux cdrecord Buffer Overflow Vulnerability

manxpl.c
Exploit for vulnerability in man (Linux)

DENIAL-OF-SERVICE

cproxy_expl.c
Exploit for CProxy 3.3 SP2 Buffer Overflow DoS Vulnerability

RFProwl.c
Exploit for Axent NetProwler Malformed IP Packets DoS Vulnerability

netprowl.casl
Exploit for Axent NetProwler Malformed IP Packets DoS Vulnerability

jolt2.c
Exploit for Microsoft Windows 9x / NT 4.0 / 2000 Fragmented IP Packets DoS Vulnerability

mdbms-exp-linux.c
Exploit for MDBMS Buffer Overflow Vulnerability

arpgen.tar.gz
Denial of service tool which demonstrates that a flood of arp requests from a spoofed ethernet and IP addresses would be a a practical attack on a local network.

Xsh0k.c
DoS against X-Windows.

cisconuke.c
Reboots cisco routers which have the web-server interface open by sending invalid data to port 80.

PASSWORD CRACKERS

ecrack-0.1.tgz
Brute force UNIX password cracker.

OTHER

shadyshell.c
Flexible, obfuscated, and lightweight UDP portshell.

snuff-v0.8.1.tar.gz
Linux packet sniffer.

hunt-1.5.tar.gz
Program that exploits vulnerabilities in TCP/IP protocol.